BUNDESREPUBLIK DEUTSCHLAND

EP04/52144

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen: 103 45 486.1

Anmeldetag: 30. September 2003

Anmelder/Inhaber: Siemens Aktiengesellschaft, 80333 München/DE

Bezeichnung: Einräumung eines Zugriffs auf ein computerbasiertes Objekt

IPC: G 06 F 21/00

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 29. September 2004
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Dzierzon

A 9161
03/00
EDV-L

Beschreibung

Einräumung eines Zugriffs auf ein computerbasiertes Objekt

Die vorliegende Erfindung betrifft ein Verfahren zur Einräumung eines Zugriffs auf ein computerbasiertes Objekt und ein Steuerungsprogramm zur Durchführung des Verfahrens.

Durch unberechtigte Benutzung von Computerprogrammen entstehen weltweit immense Schäden. Um diesem entgegenzuwirken, werden Lösungen zum Schutz von Computerprogrammen vor unberechtigter Benutzung entwickelt.

Eine Übermittlung verschlüsselter Informationen zur Aktivierung eines Computerprogramms dient einer Verhinderung von nicht autorisierten Vervielfältigungen des Computerprogramms. Entsprechende Verfahren dienen beispielsweise außerdem als technische Voraussetzung, um Computerprogramme als Produkte über E-Commerce zu vertreiben. Bei bisher bekannten Verfahren zur Aktivierung von Computerprogrammen werden Computerprogramme anhand jeweils eines Registrierungsschlüssels freigeschaltet. Für eine Freischaltung eines Computerprogramms wird der Registrierungsschlüssel, der einer Computerprogrammlizenz fest zugeordnet ist, manuell eingegeben bzw. von einem Datenträger eingespielt. Insbesondere bei einer Vielzahl von auf unterschiedlichen Computern installierten Computerprogrammen resultiert hieraus ein hoher Addministrationsaufwand, der mit personalintensiven Bedien- und Wartungsarbeiten verbunden ist.

Aus EP 1 191 419 A2 ist Verfahren bekannt, bei dem vorgebbare Funktionen eines Computerprogramms für eine wählbare Nutzungsdauer durch Modifikation eines Registrierungsschlüsselpaares freigeschaltet werden können. Das Registrierungsschlüsselpaares weist zumindest eine gegenüber Benutzerzugriffen gesperrten Teilinformation auf. Die freizuschaltenden Funktionen müssen nicht notwendigerweise bereits bei ei-

Diese Aufgabe wird erfindungsgemäß durch ein Verfahren mit den in Anspruch 1 und ein Steuerungsprogramm mit den in Anspruch 10 angegebenen Merkmalen gelöst. Vorteilhafte Ausgestaltungen der vorliegenden Erfindung sind in den abhängigen Ansprüchen angegeben.

Erfindungsgemäß resultiert ein erhöhter Schutz vor unberechtigter Benutzung von in einer Recheneinrichtung bereitgestellten Ressourcen daraus, daß als eine Voraussetzung zur Einräumung eines Zugriffs auf ein computerbasiertes Objekt eine Speicherkarte mit einem Programmcodeprozessor und eine Lizenzinformation bereitgestellt werden. Auf der Speicherkarte sind zumindest ein der Speicherkarte zugeordneter öffentlicher und privater Schlüssel sowie ein öffentlicher Schlüssel einer vertrauenswürdigen Instanz abgespeichert. Die Lizenzinformation umfaßt zumindest einen mittels des der Speicherkarte zugeordneten öffentlichen Schlüssels verschlüsselten Lizenzcode und wird an einer den Zugriff auf das computerbasierte Objekt steuernden Recheneinrichtung bereitgestellt. Der verschlüsselte Lizenzcode und eine mittels des privaten Schlüssels der vertrauenswürdigen Instanz digital signierte Angabe einer von der Speicherkarte auszuführenden Funktion zur Entschlüsselung des Lizenzcodes werden an die Speicherkarte übermittelt. Die digitale Signatur der Angabe der von der Speicherkarte auszuführenden Funktion wird nachfolgend überprüft. Bei positivem Überprüfungsergebnis wird die Funktion zur Entschlüsselung des Lizenzcodes durch die Speicherkarte ausgeführt und ein entschlüsselter Lizenzcode an die Recheneinrichtung übermittelt. Der entschlüsselte Lizenzcode wird dann zumindest temporär zum Zugriff auf das computerbasierte Objekt bereitgestellt.

Unter Recheneinrichtung sind beispielsweise ohne Beschränkung der Allgemeinheit dieses Begriffs PCs, Notebooks, Server, PDAs, Mobiltelefone, Geldautomaten, Steuerungsmodule in der Automatisierungs-, Fahrzeug-, Kommunikations- oder Medizintechnik zu verstehen - allgemein Einrichtungen, in denen Com-

seltem Lizenzcode und einem Signatur-Objekt erzeugt werden. Das Signatur-Objekt umfaßt nur einen Signaturanteil eines von der vertrauenswürdigen Instanz signierten Funktionsaufrufs zur Entschlüsselung des Lizenzcodes. Diese Ausgestaltung bietet den Vorteil, daß verfügbare Secure-Messaging-Verfahren für eine Übermittlung eines entsprechenden Funktionsaufrufs verwendet werden können. Ferner kann die Lizenzinformation zusätzlich das Signatur-Objekt umfassen, so daß eine gesicherte Bereitstellung des Signatur-Objektes gewährleistet werden kann.

Entsprechend einer weiteren vorteilhaften Ausgestaltung der vorliegenden Erfindung werden der verschlüsselte Lizenzcode und die mittels des privaten Schlüssels der vertrauenswürdigen Instanz digital signierte Angabe der von der Speicherkarte auszuführenden Funktion über eine gesicherte Kommunikationsverbindung von der Recheneinrichtung über eine Leseeinrichtung an die Speicherkarte übermittelt. Hierdurch werden Manipulationsmöglichkeiten zur unberechtigten Erlangung des Zugriffs auf das computerbasierte Objekt weiter eingeschränkt.

Vorteilhafterweise wird die digitale Signatur der Angabe der von der Speicherkarte auszuführenden Funktion anhand des öffentlichen Schlüssels der vertrauenswürdigen Instanz überprüft. Dies dient einer Verhinderung einer unberechtigten Entschlüsselung des Lizenzcodes.

Gemäß einer weiteren Ausgestaltung der vorliegenden Erfindung wird in der Recheneinrichtung eine Zufallszahl erzeugt und diese an die Speicherkarte übermittelt. Der entschlüsselte Lizenzcode wird dann mittels des der Speicherkarte zugeordneten privaten Schlüssels und der Zufallszahl digital signiert. Die digitale Signatur des entschlüsselten Lizenzcodes wird schließlich in der Recheneinrichtung anhand des der Speicherkarte zugeordneten öffentlichen Schlüssels und der Zufallszahl überprüft. Hierdurch ergibt sich ein wirksamer Wiederho-

Durch den Computer 20 werden für einen oder mehrere Benutzer Systemressourcen 22 verfügbar gemacht, die beispielsweise Programme oder Speicherbereiche mit Daten umfassen. Das hier beschriebene Verfahren zur Einräumung eines Zugriffs auf ein computerbasiertes Objekt ist grundsätzlich auf beliebige Systemressourcen anwendbar. Der Computer 20 steuert insbesondere einen Zugriff auf die Systemressourcen 22, die im vorliegenden Fall auch Software des Herstellers umfassen, welchem die vertrauenswürdige Instanz 10 zugeordnet ist. Des weiteren wird der öffentliche Schlüssel 21 der vertrauenswürdigen Instanz 10 vor Manipulation geschützt am Computer 20 bereitgestellt.

Mit dem Computer 20 ist das Smartcard-Terminal 30 über eine gesicherte Kommunikationsverbindung verbunden. Das Smartcard-Terminal 30 dient zum Informations- und Meldungsaustausch zwischen dem Computer 20 und einer in das Smartcard-Terminal 30 einführbaren Smartcard 40, die eine Speicherkarte mit einem Programmcodeprozessor darstellt. Auf der Smartcard 40 ist der öffentliche Schlüssel 41 der vertrauenswürdigen Instanz 10 sowie ein der Smartcard 40 zugeordnetes asymmetrisches Schlüsselpaar 42 abgespeichert, daß einen öffentlichen und einen privaten Schlüssel der Smartcard 40 umfaßt. Außerdem ist auf der Smartcard 40 zumindest ein Programm vorgesehen zur Ver- und Entschlüsselung unter Nutzung des asymmetrischen Schlüsselpaares 42 der Smartcard 40 und zur Verifizierung von mittels des privaten Schlüssels der vertrauenswürdigen Instanz 10 erzeugten Signaturen. Die Verifizierung von Signaturen erfolgt dabei unter Zuhilfenahme des öffentlichen Schlüssel 41 der vertrauenswürdigen Instanz 10. Darüber hinaus verfügt die Smartcard 40 über einen Zufallszahlengenerator und ist vorzugsweise konform zu IFO 7816/4.

Am Computer 20 wird eine von der vertrauenswürdigen Instanz 10 erstellte Lizenzinformation 1 bereitgestellt. Die Lizenzinformation 1 umfaßt einen mittels des der Smartcard 40 zuge-

(SM_sig_TP) erstellt, wodurch sichergestellt wird, daß die Angabe der von der Smartcard 40 auszuführenden Funktion zur Entschlüsselung des Lizenzcodes und der verschlüsselte Lizenzcode tatsächlich von der vertrauenswürdigen Instanz 10 ausgestellt worden sind.

Eine Überprüfung der digitalen Signatur der Angabe der von der Smartcard 40 auszuführenden Funktion durch die Smartcard 40 und einer Ausführung der Funktion zur Entschlüsselung des Lizenzcodes durch die Smartcard 40 bei positiven Überprüfungsergebnis zum Schutz vor Manipulationsversuchen durch Bildung eines gemeinsamen funktionalen Kontextes miteinander verknüpft. Insbesondere ist sichergestellt, daß eine Entschlüsselung des Lizenzcodes nur durch eine dafür vorgesehene Smartcard möglich ist.

Nach Ausführung der Funktion zur Entschlüsselung des Lizenzcodes (perform securitiy operation mode decrypt, angewendet auf den mittels des öffentlichen Schlüssels der Smartcard 40 verschlüsselten Lizenzcode) und Entschlüsselung wird der entschlüsselte Lizenzcode unter Anwendung von Secure-Messaging mittels einer Meldung 5 an den Computer 20 übermittelt. Zur Anwendung von Secure-Messaging wird der entschlüsselte Lizenzcode mittels des der Smartcard 40 zugeordneten privaten Schlüssels und der von dem Computer 20 erzeugten Zufallszahl digital signiert (SM_rand_sig_SC). Nach Übermittlung an den Computer 20 wird die digitale Signatur des entschlüsselten Lizenzcodes durch den Computer 20 anhand des der Speicherkarte zugeordneten öffentlichen Schlüssels und der Zufallszahl überprüft. Grundsätzlich wäre es bereits ausreichend, den entschlüsselten Lizenzcode lediglich mittels des der Smartcard 40 zugeordneten Privatschlüssels digital zu signieren und die digitale Signatur anhand des öffentlichen Schlüssels der Smartcard 40 zu überprüfen. Dies würde jedoch einen Verzicht auf den Wiederholschutz bedeuten. Je nach Anwendungsfalle und Sicherheitsanforderungen kann daher eine entsprechende Abwägung angemessener Maßnahmen vorgenommen werden.

Die Anwendung der vorliegenden Erfindung ist nicht auf das hier beschriebene Ausführungsbeispiel beschränkt.

chen Schlüssels der vertrauenswürdigen Instanz überprüft wird.

3. Verfahren nach einem der Ansprüche 1 oder 2,
bei dem die Lizenzinformation zusätzlich den der Speicherkarte zugeordneten öffentlichen Schlüssel umfaßt, bei dem der entschlüsselte Lizenzcode mittels des der Speicherkarte zugeordneten privaten Schlüssels digital signiert wird, und bei dem die digitale Signatur des entschlüsselten Lizenzcodes in der Recheneinrichtung anhand des der Speicherkarte zugeordneten öffentlichen Schlüssels überprüft wird.

4. Verfahren nach einem der Ansprüche 1 bis 3,
bei dem die mittels des privaten Schlüssels der vertrauenswürdigen Instanz digital signierte Angabe der von der Speicherkarte auszuführenden Funktion zur Entschlüsselung des Lizenzcodes in der Recheneinrichtung aus dem verschlüsseltem Lizenzcode und einem Signatur-Objekt erzeugt wird, das nur einen Signaturanteil eines von der vertrauenswürdigen Instanz signierten Funktionsaufrufs zur Entschlüsselung des Lizenzcodes umfaßt.

5. Verfahren nach Anspruch 4,
bei dem die Lizenzinformation zusätzlich das Signatur-Objekt umfaßt.

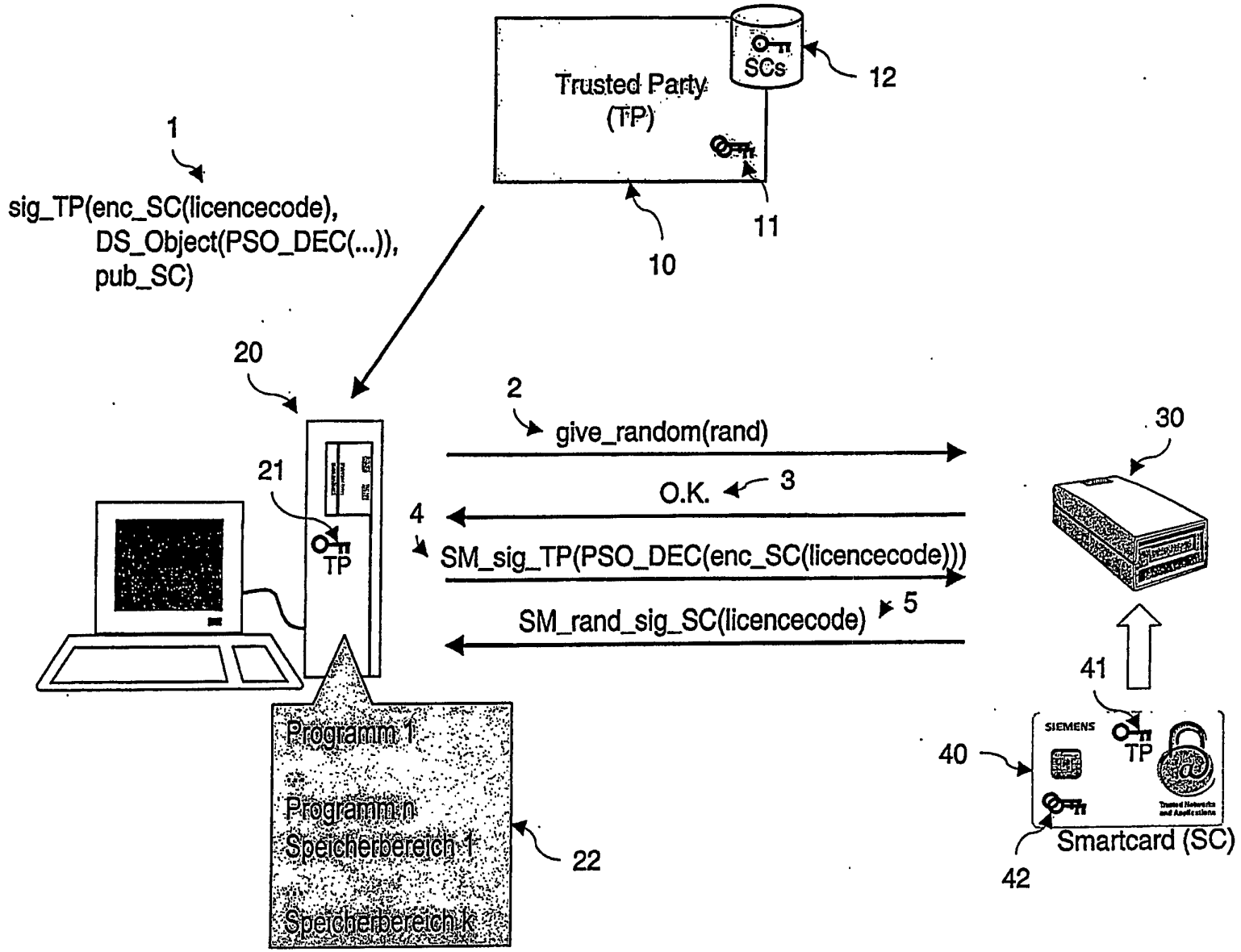
6. Verfahren nach einem der Ansprüche 1 bis 5,
bei dem der verschlüsselte Lizenzcode und die mittels des privaten Schlüssels der vertrauenswürdigen Instanz digital signierte Angabe der von der Speicherkarte auszuführenden Funktion über eine gesicherte Kommunikationsverbindung von der Recheneinrichtung über eine Leseeinrichtung an die Speicherkarte übermittelt werden.

7. Verfahren nach einem der Ansprüche 1 bis 6,

- der entschlüsselte Lizenzcode zumindest temporär zum Zugriff auf das computerbasierte Objekt durch die Recheneinrichtung bereitgestellt wird,

wenn das Steuerungsprogramm in der Recheneinrichtung abläuft.

FIG.


Trusted Party
(TP)
SCs
12
11
10
1
sig_TP(enc_SC(licencecode),
DS_Object(PSO_DEC(...)),
pub_SC)
20
21
TP
2
give_random(rand)
O.K.
3
4
SM_sig_TP(PSO_DEC(enc_SC(licencecode)))
SM_rand_sig_SC(licencecode)
5
30
41
SIEMENS
TP
40
Smartcard (SC)
42
Programm 1
Programm n
Speicherbereich 1
Speicherbereich k
22